



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/795,922	03/08/2004	Fatih Comlekoglu		1816

7590  
Scot A. Reader, P.C  
Suite 224  
1320 Pearl St.  
Boulder, CO 80302

03/03/2009

EXAMINER
----------

JOHNSON, CARLTON

ART UNIT	PAPER NUMBER
----------	--------------

2436

MAIL DATE	DELIVERY MODE
-----------	---------------

03/03/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/795,922	<b>Applicant(s)</b> COMLEKOGLU ET AL.	
	<b>Examiner</b> CARLTON V. JOHNSON	<b>Art Unit</b> 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 01 December 2008.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 29-48, 55 and 56 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 29-48, 55, 56 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

### **DETAILED ACTION**

1. This action is responding to application amendments filed on 12-1-2008.
2. Claims **29 - 48, 55, 56** are pending. Claims **29, 42, 55** have been amended. Claims **1 - 28, 49 - 54** have been cancelled. Claims **29, 42, 55** are independent. This application was filed on 3-8-2004.

### ***Response to Arguments***

3. Applicant's arguments filed 12-1-2008 have been fully considered but they were not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, "Purging Temporary Memory on the End System in Response to Detected Termination of the VPN Connection Whereby Malicious Code Written to Temporary Memory While Permitting VPN Access is Eradicated from the End System. (see Remarks Page 8)

The Harrison prior art discloses that data can be deleted from the end system after termination of a VPN or secure communication session. (see Harrison col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system); col. 9, lines 6-13: capabilities to delete data after VPN or secure communications terminated)

3.2 Applicant argues that the referenced prior art does not disclose, "Filtering Detected Traffic Received on the End System that Is Not on the VPN Connection". (see Remarks Page 11)

The Aiello prior art discloses VPN data packet monitoring to detect non-VPN traffic. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module)

3.3 Applicant argues that the referenced prior art does not disclose, a Plurality of Memories "Consisting of" at Least One Write-Protected Permanent Memory and at Least One Temporary Memory. (see Remarks Page 12)

The Harrison prior art discloses write protected memory. The claim limitation discloses write protected not write disabled memory. The term "write protected" denotes access controls over entities that limit access and write capabilities. (Harrison col. 5, lines 38-45: authentication credentials to authenticate access to data repository; col. 12, lines 12-14: prevent unauthorized accessing data stored by another; limits which repositories an applet can access)

3.4 Applicant argues that the referenced prior art does not disclose, Harrison does not operate in a VPN environment. (see Remarks Page 9)

The Harrison prior art operates within a secure environment which is equivalent to a VPN type environment (secure communications environment). (see Harrison col. 4, lines 60-66: allow untrusted applets to have access to persistent storage without compromising the integrity or security of client systems; insuring storage integrity and security)

Art Unit: 2436

3.5 Applicant argues that the referenced prior art does not disclose, Harrison does not take action in response to termination of VPN connection. (see Remarks Page 10)

The Harrison prior art discloses that data can be deleted from the end system after termination of a VPN or secure communications session. (see Harrison col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system); col. 9, lines 6-13: capability to delete data after VPN or secure communications terminated)

3.6 Aiello prior art discloses VPN data packet monitoring to detect non-VPN traffic. (see Aiello paragraph [0008], lines 1-8: filter module filters packets passing through the tunnel that are not packets associated with the tunnel (non-VPN traffic is filtered); paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module)

Harrison prior art discloses a prohibition of permanent writing on the client system of a VPN tunnel. (see Harrison col. 6, lines 28-31: provide client side persistent storage for untrusted clients; col. 4, lines 60-66: access to storage for client system; storage integrity and security if removed from programmer; col. 5, lines 46-48: data repository size; col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system))

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims **29 - 48, 55, 56** are rejected under 35 U.S.C. 103 (a) as being unpatentable over Aiello et al. (US PG PUB No. **20040123139**) in view of **Harrison et al.** (US Patent No. **6,691,113**) and further in view of **Cheline et al.** (US PG PUB No. **20030041136**).

**Regarding Claim 29**, Aiello discloses a method for reducing vulnerability of a Virtual Private Network (VPN) protected network to attack by an end system, comprising the steps of:

while permitting the access:

- b) continuously monitoring on the end system; (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module)
- c) continuously monitoring on the end system for traffic on the end system and filtering detected traffic inbound to the end system that is not on the VPN connection; (see Aiello paragraph [0020], lines 3-7: packets are filtered and monitored to detect packets that do not meet security protocol requirements

Art Unit: 2436

- for a secure channel; paragraph [0009], lines 1-6: detect non-VPN traffic)
- d) continuously monitoring on the end system for termination of the VPN connection. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module (data exchange indicating session termination))

Aiello does not specifically disclose attempted writes to the end system and preventing attempted writes to permanent memory on the end system.

However, Harrison discloses attempted writes to the end system, preventing detected attempted writes to permanent memory on the end system and purging temporary memory on the end system in response to detected termination of the VPN connection whereby malicious code written to temporary memory while permitting the access is eradicated from the end system. (see Harrison col. 6, lines 28-31: provide client side persistent storage for untrusted clients; col. 4, lines 60-66: access to storage for client system; storage integrity and security if removed from programmer; col. 5, lines 46-48: data repository size; col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system); data written can be removed from system after VPN or secure communications session terminated)

It would have been obvious to one of ordinary skill in the art to modify Aiello for attempted writes to the end system, preventing detected attempted writes to permanent memory and purging temporary memory on the end system as taught by

Art Unit: 2436

Harrison. One of ordinary skill in the art would have been motivated to employ the teachings of Harrison in order to allow untrusted applets to have access to persistent storage without compromising the integrity of the client computer system. (see Harrison col. 4, lines 60-62: “ ... *A benefit of the present invention is that it allows untrusted applets to have access to persistent storage without compromising the integrity of the client computer system.* ... ”)

Aiello discloses wherein permitting access by an end system to a VPN protected network on at least one VPN connection for a user of the end system to the VPN protected network. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose authenticating a user of the end system.

However, Cheline discloses:

- a) authenticating a user of the end system; (see Cheline paragraph [0049], lines 1-10: user authenticated; paragraph [0049], lines 11-14: permit access (encrypted packets transferred) to end system)

It would have been obvious to one of ordinary skill in the art to modify Aiello for authenticating a user of the end system as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5: “ ... *Using the above, a less complex, less efficient, and less costly method for configuring a VPN is provided,*



Art Unit: 2436

*thereby allowing the resources of a service provider to be redirected to areas other than manually configuring the system. ... “)*

**Regarding Claims 30, 43,** Aiello discloses the method, and system of claims 29, 42, wherein continuous monitoring. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose the step of attempted writes to the end system further comprising redirecting to temporary memory detected attempted writes to permanent memory. However, Harrison discloses wherein the step of attempted writes to the end system further comprises redirecting to temporary memory detected attempted writes to permanent memory. (see Harrison col. 6, lines 28-31: provide client side persistent storage for untrusted clients; col. 4, lines 60-66: access to storage for client system; storage integrity and security if removed from programmer : col. 5, lines 46-48: data repository size; col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system))

It would have been obvious to one of ordinary skill in the art to modify Aiello for attempted writes to permanent memory redirected to temporary memory as taught by Harrison. One of ordinary skill in the art would have been motivated to employ the teachings of Harrison in order to allow untrusted applets to have access to persistent storage without compromising the integrity of the client computer system. (see Harrison col. 4, lines 60-62)

**Regarding Claims 31, 44,** Aiello discloses the method, end system of claims 29, 42 wherein the step of continuously monitoring for traffic on the end system comprises filtering detected traffic outbound from the end system that is not on the VPN connection. (see Aiello paragraph [0009], lines 1-6: monitor module detects non-VPN packets)

**Regarding Claims 32, 45,** Aiello discloses the method, end system of claims 29, 42. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose before permitting the access, the step of denying network access except for performing user authentication. However, Cheline discloses further comprising, before permitting the access, the step of denying network access except for performing user authentication. (see Cheline paragraph [0043], lines 1-8; paragraph [0069], lines 4-11: access only after user authentication)

It would have been obvious to one of ordinary skill in the art to modify Aiello for the step of denying network access except for performing user authentication as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

Art Unit: 2436

**Regarding Claim 33**, Aiello discloses the method of claim 29, wherein the monitoring steps are performed by the end system. (see Aiello paragraph [0010], lines 1-4: module or filter modules are co-located on one or more of the tunnel hosts (end systems))

**Regarding Claim 34**, Aiello discloses the method of claim 33, wherein the monitoring steps are performed by software having instructions executable by a processor. (see Aiello paragraph [0054], lines 1-3: crypto modules and monitors (software modules) can be done in hardware or software)

**Regarding Claims 35, 46**, Aiello discloses the method, end system of claims 34, 42, wherein the software is embedded in permanent memory. (see Aiello paragraph [0054], lines 1-3: monitors done (implemented) in software; paragraph [0048], lines 7-14: tunnels hosts include various computers and workstations running any number of operation systems; portable computers (permanent memory used to hold operational software for portable computers))

**Regarding Claims 36, 47**, Aiello discloses the method, end system of claims 35, 42, wherein the software. (see Aiello paragraph [0054], lines 1-3: monitors done (implemented) in software; paragraph [0048], lines 7-14: tunnels hosts include various computers and workstations running any number of operation systems; portable computers) Aiello does not specifically disclose being adapted to inhibit modification of the software by the user. However, Harrison discloses wherein adapted to inhibit

Art Unit: 2436

modification of the software by the user. (see Harrison col. 6, lines 28-31: provide client side persistent storage for untrusted clients; col. 4, lines 60-66: access to storage for client system; storage integrity and security if removed from programmer : col. 5, lines 46-48: data repository size; col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system; no modification of software on permanent storage by user))

It would have been obvious to one of ordinary skill in the art to modify Aiello whereby adapted to inhibit modification of the software by the user as taught by Harrison. One of ordinary skill in the art would have been motivated to employ the teachings of Harrison in order to allow untrusted applets to have access to persistent storage without compromising the integrity of the client computer system. (see Harrison col. 4, lines 60-62)

**Regarding Claim 37**, Aiello discloses the method of claim 29. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose the step of monitoring for termination by logging-off the user in response to detected termination of the VPN connection. However, Cheline discloses wherein the step of monitoring for termination further comprises logging-off the user in response to detected termination of the VPN connection. (see Cheline paragraph [0076], lines 1-5: relogin, restarting end system)

Art Unit: 2436

It would have been obvious to one of ordinary skill in the art to modify Aiello for logging-off the user in response to detected termination of the VPN connection as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

**Regarding Claim 38**, Aiello discloses the method of claim 29, wherein the step of monitoring for termination. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose rebooting the end system in response to detected termination of the VPN connection. However, Cheline discloses wherein further comprising rebooting the end system in response to detected termination of the VPN connection. (see Cheline paragraph [0076], lines 1-5: relogin, restarting end system)

It would have been obvious to one of ordinary skill in the art to modify Aiello to reboot the end system in response to detected termination of the VPN connection as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

Art Unit: 2436

**Regarding Claim 39**, Aiello discloses the method of claim 29, wherein the step of monitoring for termination. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose shutting down the end system in response to detected termination of the VPN connection. However, Cheline discloses wherein further comprises shutting down the end system in response to detected termination of the VPN connection. (see Cheline paragraph [0076], lines 10-14: VPN disconnected, tunnel torn down)

It would have been obvious to one of ordinary skill in the art to modify Aiello for shutting down the end system in response to detected termination of the VPN connection as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

**Regarding Claim 40**, Aiello discloses the method of claim 29. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose flash memory. However, Cheline discloses wherein permanent memory comprises a flash memory. (see Cheline paragraph [0047], lines 16-17; paragraph [0057], lines 3-5: flash memory)

It would have been obvious to one of ordinary skill in the art to modify Aiello for

Art Unit: 2436

permanent memory comprising a flash memory as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

**Regarding Claim 41**, Aiello discloses the method of claim 29. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module) Aiello does not specifically disclose a random access memory (RAM) disk. However, Cheline discloses wherein temporary memory comprises a random access memory (RAM) disk. (see Cheline paragraph [0047], lines 1-10: permanent type memory (RAM) for program such as operating system)

It would have been obvious to one of ordinary skill in the art to modify Aiello for a random access memory (RAM) disk as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

**Regarding Claim 42**, Aiello discloses a VPN capable end system, comprising:

software stored on the permanent memory, the software having instructions executable by the processor while the end system is permitted access to a VPN protected network on at least one VPN connection, continuously monitor for

Art Unit: 2436

attempted writes to the end system and to continuously monitor for traffic on the end system and filter detected traffic inbound to the end system that is not on the VPN connection. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module)

Aiello does not specifically disclose preventing detected attempted writes to the permanent memory and purging temporary memory.

However, Harrison discloses:

d) preventing detected attempted writes to the permanent memory and purging the temporary memory. (see Harrison col. 6, lines 28-31: provide client side persistent storage for untrusted clients; col. 4, lines 60-66: access to storage for client system; storage integrity and security if removed from programmer : col. 5, lines 46-48: data repository size; col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system))

It would have been obvious to one of ordinary skill in the art to modify Aiello for preventing detected attempted writes to permanent memory and purging temporary memory as taught by Harrison. One of ordinary skill in the art would have been motivated to employ the teachings of Harrison in order to allow untrusted applets to have access to persistent storage without compromising the integrity of the client computer system. (see Harrison col. 4, lines 60-62)

Aiello does not specifically disclose at least one permanent memory, at least one



Art Unit: 2436

temporary memory and at least one processor coupled to the permanent memory and the temporary memory.

However, Cheline discloses:

- a) at least one permanent memory; (see Cheline paragraph [0047], lines 1-10: permanent type memory for program such as operating system)
- b) at least one temporary memory; (see Cheline paragraph [0058], line 1: temporary memory)
- c) at least one processor coupled to the permanent memory and the temporary memory; (see Cheline paragraph [0047], lines 1-3: processor, interface (bus) between components)
- d) termination of the VPN connection whereby malicious code written to temporary memory while permitting the access is eradicated from the end system. (see Cheline paragraph [0071], lines 1-3: VPN access to end system enabled; paragraph [0076], lines 1-5: logoff user, VPN disconnected or inactive; paragraph [0076], lines 10-14: VPN disconnected, tunnel torn down; data written can be removed from system after VPN or secure communications session terminated)

It would have been obvious to one of ordinary skill in the art to modify Aiello for at least one permanent memory, at least one temporary memory and at least one processor coupled to the permanent memory and the temporary memory and termination of the VPN connection as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN

is provided. (see Cheline paragraph [0017], lines 1-5)

**Regarding Claim 48**, Aiello discloses the end system of claim 42, wherein the software further has instructions executable by the processor. (see Aiello paragraph [0054], lines 1-3: monitors can be done in software (instructions)) Aiello does not specifically disclose that the end system is not permitted the access to facilitate authentication of a user of the end system to the VPN protected network. However, Cheline discloses wherein while the end system is not permitted the access to facilitate authentication of a user of the end system to the VPN protected network. (see Cheline paragraph [0043], lines 1-8; paragraph [0069], lines 4-11: access only after user authentication)

It would have been obvious to one of ordinary skill in the art to modify Aiello where the end system is not permitted the access to facilitate authentication of a user of the end system as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

**Regarding Claim 55**, Aiello discloses a VPN capable end system, comprising:

- a) a plurality of memories consisting of at least one write-protected permanent memory and at least one temporary memory (see Cheline paragraph [0047], lines 1-10: permanent type memory for program such as operating system; paragraph [0058], line 1: temporary memory); at least one processor coupled to

Art Unit: 2436

the memories (see Cheline paragraph [0047], lines 1-3: processor, interface (bus) between components);

- b) software (see Aiello paragraph [0054], lines 1-3: monitor implemented in software; paragraph [0048, lines 7-14: tunnel hosts include various computers) stored in the permanent memory, the software having instructions executable by the processor while the end system is permitted access to a VPN protected network on at least one VPN connection to continuously monitor traffic on the end system and filter detected traffic received on the end system that is not on the VPN connection, and to continuously monitor for termination of the VPN connection whereby malicious code written to temporary memory while permitting the access is eradicated from the end system. (see Aiello paragraph [0007], lines 1-6; paragraph [0009], lines 1-5: monitor data exchange over a secure channel such as a VPN tunnel, can be monitored to detect potential security breaches; monitor module; paragraph [0009], lines 1-6: detect non-VPN traffic; data written can be removed from system after VPN or secure communications session terminated)

Aiello does not specifically disclose attempted writes to the end system and preventing detected attempted writes to permanent memory and purging temporary memory. However, Harrison discloses wherein monitor for attempted writes to the end system and prevent detected attempted writes to the permanent memory and purge the temporary memory. (see Harrison col. 6, lines 28-31: provide client side persistent storage for untrusted clients; col. 4, lines 60-66: access to storage for

Art Unit: 2436

client system; storage integrity and security if removed from programmer; col. 5, lines 46-48: data repository size; col. 5, lines 52-55: expiration of predefined time period; temporary file (no writes to permanent storage on client system))

It would have been obvious to one of ordinary skill in the art to modify Aiello for attempted writes to the end system and preventing detected attempted writes to permanent memory and purging temporary memory as taught by Harrison. One of ordinary skill in the art would have been motivated to employ the teachings of Harrison in order to allow untrusted applets to have access to persistent storage without compromising the integrity of the client computer system. (see Harrison col. 4, lines 60-62)

Aiello does not specifically disclose monitoring for termination of the VPN connection. However, Cheline discloses wherein monitoring for termination of the VPN connection. (see Cheline paragraph [0076], lines 1-5: logoff user, VPN disconnected or inactive; paragraph [0076], lines 10-14: VPN disconnected, tunnel torn down)

It would have been obvious to one of ordinary skill in the art to modify Aiello to monitor for termination of the VPN connection as taught by Cheline. One of ordinary skill in the art would have been motivated to employ the teachings of Cheline in order to provide a less complex, less efficient, and less costly method for configuring a VPN is provided. (see Cheline paragraph [0017], lines 1-5)

**Regarding Claim 55**, Aiello discloses the end system of claim 55, wherein the software

Art Unit: 2436

further has instructions executable by the processor while the end system is permitted the access to redirect to the temporary memory detected attempted writes to the permanent memory. (see Aiello paragraph [0054], lines 1-3: monitors done (implemented) in software; paragraph [0048], lines 7-14: tunnels hosts include various computers and workstations running any number of operation systems; portable computers (permanent memory used to hold software portable computers))

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-

Art Unit: 2436

270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/  
Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson  
Examiner  
Art Unit 2436

CVJ  
February 17, 2009

Application/Control Number: 10/795,922  
Art Unit: 2436

Page 22